UNIVERSIDAD CARLOS III DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

INGENIERÍA TÉCNICA DE TELECOMUNICACIÓN

ESPECIALIDAD: TELEMÁTICA

PROYECTO FINAL DE CARRERA

VERIFICADOR MÓVIL DE DOCUMENTOS DE TRÁNSITO

AUTOR: Javier Hernández Fisac
TUTOR: Juan Manuel Estévez Tapiador

26 de junio de 2015

Contenido

Contenido

Motivación

Motivación

- Tránsito de personas a nivel doméstico o entre diferentes países.

Motivación

- Tránsito de personas a nivel doméstico o entre diferentes países.
- Necesidad de mecanismos electrónicos seguros y portables de control.

Motivación

- Tránsito de personas a nivel doméstico o entre diferentes países.
- Necesidad de mecanismos electrónicos seguros y portables de control.
- Machine Readable Travel Document (MRTD) de ICAO con seguridad lógica y biometría.

Motivación

- Tránsito de personas a nivel doméstico o entre diferentes países.
- Necesidad de mecanismos electrónicos seguros y portables de control.
- Machine Readable Travel Document (MRTD) de ICAO con seguridad lógica y biometría.
- DNIe español con seguridad lógica y biometría.

Motivación

- Tránsito de personas a nivel doméstico o entre diferentes países.
- Necesidad de mecanismos electrónicos seguros y portables de control.
- Machine Readable Travel Document (MRTD) de ICAO con seguridad lógica y biometría.
- DNIe español con seguridad lógica y biometría.

Ejemplo: ABC System en los aeropuertos españoles

Contenido

Objetivos

- Solución móvil.

Objetivos

- Solución móvil.
- Verificación lógica de MRTD de ICAO (inalámbrica).

Objetivos

- Solución móvil.
- Verificación lógica de MRTD de ICAO (inalámbrica).
- Verificación lógica de DNIe (por contactos).

Objetivos

- Solución móvil.
- Verificación lógica de MRTD de ICAO (inalámbrica).
- Verificación lógica de DNIe (por contactos).
- Cotejo facial y dactilar.

Objetivos

- Solución móvil.
- Verificación lógica de MRTD de ICAO (inalámbrica).
- Verificación lógica de DNIe (por contactos).
- Cotejo facial y dactilar.
- Datos policiales del documento y el titular.

Contenido

Machine Readable Travel Document (MRTD)

Machine Readable Travel Document (MRTD)

- Basado en el documento 9303 de la International Civil Aviation Organization (ICAO).

Machine Readable Travel Document (MRTD)

- Basado en el documento 9303 de la International Civil Aviation Organization (ICAO).
- Información almacenada en una Estructura lógica de los datos (LDS) mediante Data Groups (DGs).

Machine Readable Travel Document (MRTD)

- Basado en el documento 9303 de la International Civil Aviation Organization (ICAO).
- Información almacenada en una Estructura lógica de los datos (LDS) mediante Data Groups (DGs).

Machine Readable Travel Document (MRTD) (II)

Mecanismos de seguridad

Mecanismo	Objetivo	Técnica	ICAO	UE

Machine Readable Travel Document (MRTD) (II)
Mecanismos de seguridad

Mecanismo	Objetivo	Técnica	ICAO	UE
BAC	Confidencialidad	Autenticación y Canales Seguros	Opcional	Obligatorio

Machine Readable Travel Document (MRTD) (II)

Mecanismos de seguridad

Mecanismo	Objetivo	Técnica	ICAO	UE
BAC	Confidencialidad	Autenticación y Canales Seguros	Opcional	Obligatorio
PA	Autenticidad	Firma digital	Obligatorio	Obligatorio

Machine Readable Travel Document (MRTD) (II)
Mecanismos de seguridad

Mecanismo	Objetivo	Técnica	ICAO	UE
BAC	Confidencialidad	Autenticación y Canales Seguros	Opcional	Obligatorio
PA	Autenticidad	Firma digital	Obligatorio	Obligatorio
AA	Originalidad	Reto-Respuesta	Opcional	Opcional

Machine Readable Travel Document (MRTD) (II)
Mecanismos de seguridad

Mecanismo	Objetivo	Técnica	ICAO	UE
BAC	Confidencialidad	Autenticación y Canales Seguros	Opcional	Obligatorio
PA	Autenticidad	Firma digital	Obligatorio	Obligatorio
AA	Originalidad	Reto-Respuesta	Opcional	Opcional
EAC	C/A/O	Autenticación mediante PKI	Opcional	Obligatorio con huella

MRTD Basic Access Control (BAC)

MRTD Basic Access Control (BAC)

- Garantiza el contacto visual con el dispositivo de inspección.

MRTD Basic Access Control (BAC)

- Garantiza el contacto visual con el dispositivo de inspección.
- Opcional según ICAO, pero **obligatorio** según la Unión Europea.

MRTD Basic Access Control (BAC)

- Garantiza el contacto visual con el dispositivo de inspección.
- Opcional según ICAO, pero **obligatorio** según la Unión Europea.
- Permite acceder a datos poco sensibles del pasaporte (DG1, DG2).

MRTD Basic Access Control (BAC)

- Garantiza el contacto visual con el dispositivo de inspección.
- Opcional según ICAO, pero **obligatorio** según la Unión Europea.
- Permite acceder a datos poco sensibles del pasaporte (DG1, DG2).

Proceso de Control de Acceso Básico

- Lectura visual de la MRZ.
- Extracción del número del documento, fecha de nacimiento y fecha de caducidad.
- Generación del par de claves de cifrado (K_{ENC}) y autenticación (K_{MAC}) del canal.

MRTD Passive Authentication (PA)

MRTD Passive Authentication (PA)

- Permite verificar que los DGs no han sido alterados desde la expedición del documento.

MRTD Passive Authentication (PA)

- Permite verificar que los DGs no han sido alterados desde la expedición del documento.
- Utiliza el Security Object Data (SOD), DG que contiene los hashes de todos los DGs.

MRTD Passive Authentication (PA)

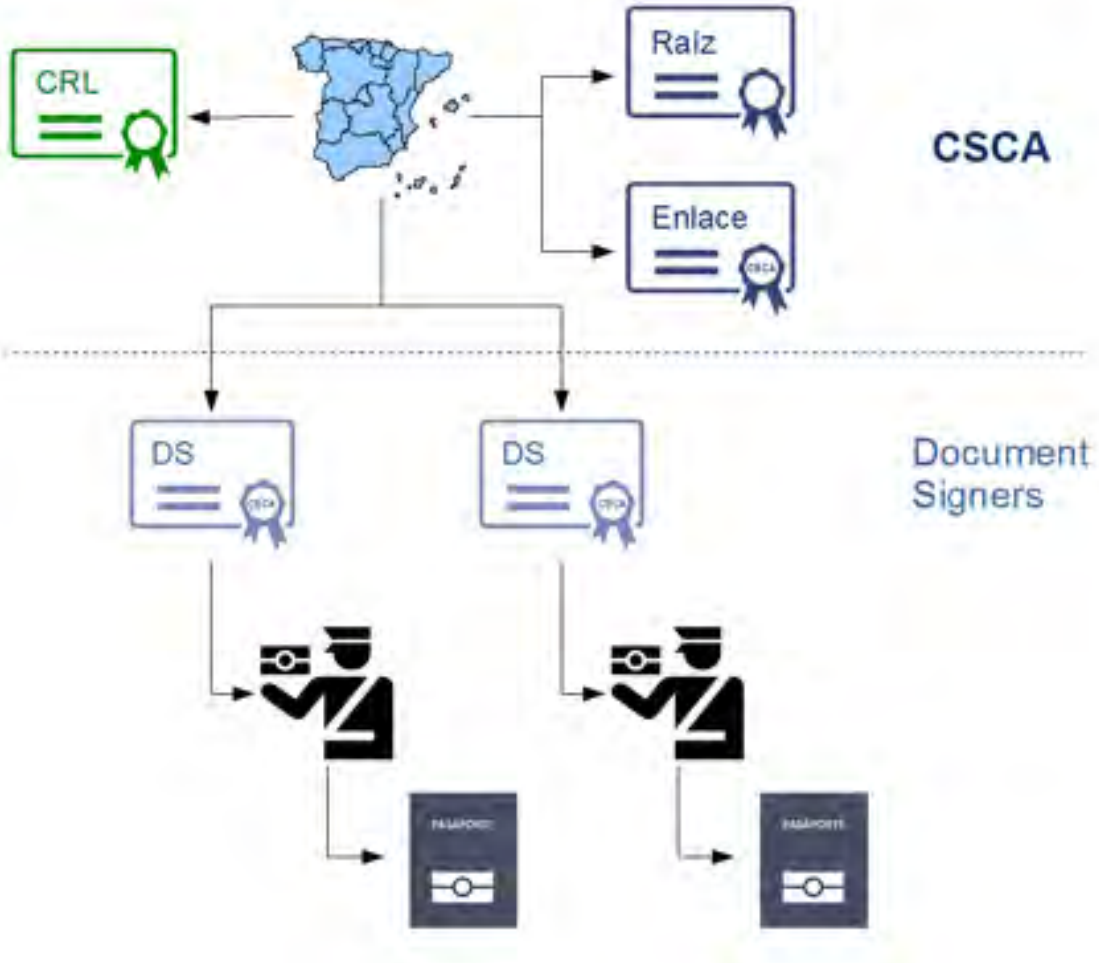
- Permite verificar que los DGs no han sido alterados desde la expedición del documento.
- Utiliza el Security Object Data (SOD), DG que contiene los hashes de todos los DGs.
- El SOD es firmado con un certificado Country Signing Certification Authority (CSCA).

MRTD Passive Authentication (PA)

- Permite verificar que los DGs no han sido alterados desde la expedición del documento.
- Utiliza el Security Object Data (SOD), DG que contiene los hashes de todos los DGs.
- El SOD es firmado con un certificado Country Signing Certification Authority (CSCA).
- No se puede asegurar que los datos no hayan sido clonados.

MRTD Passive Authentication (PA) (II)

Jerarquía Country Signing Certification Authority (CSCA)



MRTD Passive Authentication (PA) (III)

Proceso de Autenticación Pasiva

- Leer el SOD del MRTD.
- Obtener el certificado de DS firmado por la CSCA.
- Verificar el DS con la CSCAs correspondiente al país.
- Calcular los hashes de los DGs.
- Verificar la firma del SOD.
- Comparar la firma calculada, con la obtenida del pasaporte.

MRTD Active Authentication (AA)

MRTD Active Authentication (AA)

- Previene la clonación de todos los datos del documento.

MRTD Active Authentication (AA)

- Previene la clonación de todos los datos del documento.
- Utiliza un par de claves únicos del dispositivo.

MRTD Active Authentication (AA)

- Previene la clonación de todos los datos del documento.
- Utiliza un par de claves únicos del dispositivo.
- Clave pública del chip almacenada en el DG15 protegida por la Passive Authentication (PA).

MRTD Active Authentication (AA)

- Previene la clonación de todos los datos del documento.
- Utiliza un par de claves únicos del dispositivo.
- Clave pública del chip almacenada en el DG15 protegida por la Passive Authentication (PA).
- Clave privada en zona de memoria segura del chip.

MRTD Active Authentication (AA)

- Previene la clonación de todos los datos del documento.
- Utiliza un par de claves únicos del dispositivo.
- Clave pública del chip almacenada en el DG15 protegida por la Passive Authentication (PA).
- Clave privada en zona de memoria segura del chip.
- Opcional según ICAO.

MRTD Active Authentication (AA)

- Previene la clonación de todos los datos del documento.
- Utiliza un par de claves únicos del dispositivo.
- Clave pública del chip almacenada en el DG15 protegida por la Passive Authentication (PA).
- Clave privada en zona de memoria segura del chip.
- Opcional según ICAO.

Proceso de Autenticación Activa

- Se obtiene la clave pública del chip leyendo el DG15.
- Se envía un reto de firma al MRTD.
- El MRTD firma el reto con su clave privada y lo devuelve al sistema de inspección.
- Se verifica que el reto enviado es el mismo que el recibido.

MRTD Extended Access Control (EAC)

MRTD Extended Access Control (EAC)

- Garantiza la autenticación mutua entre el documento y el sistema de inspección.

MRTD Extended Access Control (EAC)

- Garantiza la autenticación mutua entre el documento y el sistema de inspección.
- Proceso en dos fases, Chip Authentication (CA) y Terminal Authentication (TA).

MRTD Extended Access Control (EAC)

- Garantiza la autenticación mutua entre el documento y el sistema de inspección.
- Proceso en dos fases, Chip Authentication (CA) y Terminal Authentication (TA).
- Basada en el uso de certificados CVCA.

MRTD Extended Access Control (EAC)

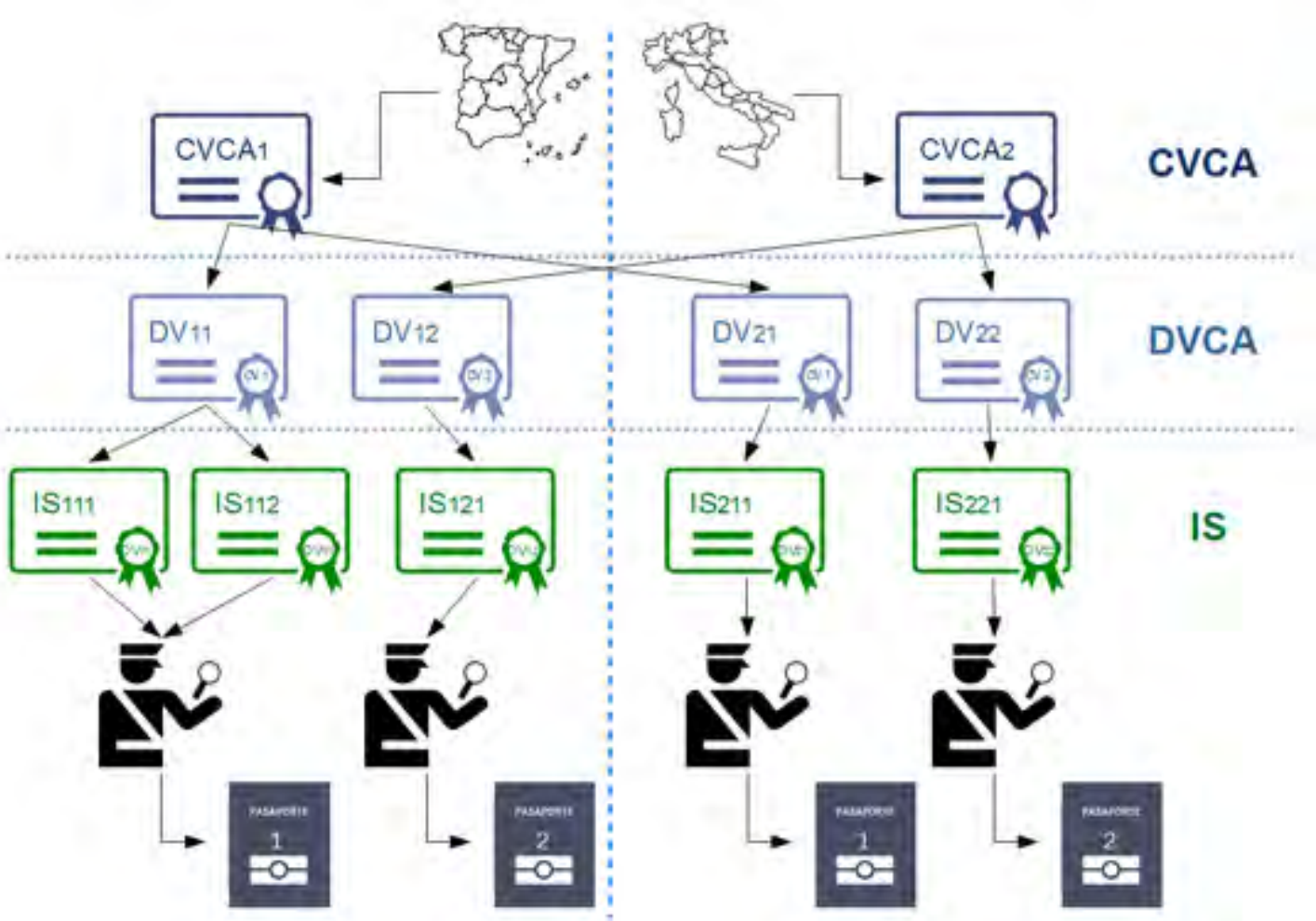
- Garantiza la autenticación mutua entre el documento y el sistema de inspección.
- Proceso en dos fases, Chip Authentication (CA) y Terminal Authentication (TA).
- Basada en el uso de certificados CVCA.
- Permite acceder a datos sensibles del pasaporte (DG3).

MRTD Extended Access Control (EAC)

- Garantiza la autenticación mutua entre el documento y el sistema de inspección.
- Proceso en dos fases, Chip Authentication (CA) y Terminal Authentication (TA).
- Basada en el uso de certificados CVCA.
- Permite acceder a datos sensibles del pasaporte (DG3).
- Ideado por la UE y **obligatorio** en los MRTD con información biométrica.

MRTD Extended Access Control (EAC) (II)

Jerarquía Country Verifying Certificate Authority (CVCA)



MRTD Extended Access Control (EAC) (III)
Chip Authentication (CA)

Proceso de Autenticación de Chip (CA)

- El sistema de inspección lee la clave pública del MRTD del DG14.
- Se generan un par de claves efímeras Diffie-Hellman (DH) o Elliptic Curve Diffie-Hellman (ECDH) y se envía la clave pública al MRTD.
- Ambos, el MRTD y el sistema de inspección, derivan nuevas claves de sesión simétricas (K_{ENC}, K_{MAC}) mediante la utilización del secreto compartido generado.

MRTD Extended Access Control (EAC) (IV)
Terminal Authentication (TA)

Proceso de Autenticación de Terminal (TA)

Proceso de Autenticación de Terminal (TA)

- **Verificación de la cadena de certificados**
  - El terminal accede al Certification Authority Reference (CAR) de la CVCA del emisor del documento.
  - Se envía secuencialmente la jerarquía de la CVCA hasta el IS correspondiente.
  - El MRTD verifica la cadena con la clave pública de la CVCA.
  - Se actualizan los datos del CAR y certificado CVCAs en el MRTD si aplica.

MRTD Extended Access Control (EAC) (IV)
Terminal Authentication (TA)

Proceso de Autenticación de Terminal (TA)

- **Verificación de la cadena de certificados**
  - El terminal accede al Certification Authority Reference (CAR) de la CVCA del emisor del documento.
  - Se envía secuencialmente la jerarquía de la CVCA hasta el IS correspondiente.
  - El MRTD verifica la cadena con la clave pública de la CVCA.
  - Se actualizan los datos del CAR y certificado CVCAs en el MRTD si aplica.
- **Comprobación de la validez del IS**
  - El MRTD envía al sistema de inspección un reto.
  - El sistema de inspección cifra el reto con la clave privada del IS, y lo envía al MRTD.
  - El MRTD descifra el reto con la clave pública que recibió con la cadena de certificados y compara con el reto enviado.

Contenido

DNIe

DNIe

- Emitido por la Dirección General de la Policía de España.

DNIe

- Emitido por la Dirección General de la Policía de España.
- Acredita la identidad, datos personales y nacionalidad española de su titular.

DNIe

- Emitido por la Dirección General de la Policía de España.
- Acredita la identidad, datos personales y nacionalidad española de su titular.
- Chip Integrated Circuit Card (ICC), capaz de guardar y procesar de forma segura información.

DNIe

- Emitido por la Dirección General de la Policía de España.
- Acredita la identidad, datos personales y nacionalidad española de su titular.
- Chip Integrated Circuit Card (ICC), capaz de guardar y procesar de forma segura información.
- Permite firmas digitales, acceso a servicios en Internet e identificación electrónica.

DNIe (II)
Estructura de datos

DNIe (II)
Estructura de datos

Zona pública accesible en lectura sin restricciones

- Certificado de Autoridad de Certificación intermedia emisora.
- Claves Diffie-Hellman.
- Certificado X.509 de componente.

DNIe (II)
Estructura de datos

Zona pública accesible en lectura sin restricciones

- Certificado de Autoridad de Certificación intermedia emisora.
- Claves Diffie-Hellman.
- Certificado X.509 de componente.

Zona privada accesible por el ciudadano con PIN

- Certificado de Firma, para la realización de firmas electrónicas.
- Certificado de Autenticación, para autenticación electrónica en Internet.

DNIe (II)
Estructura de datos

Zona pública accesible en lectura sin restricciones

- Certificado de Autoridad de Certificación intermedia emisora.
- Claves Diffie-Hellman.
- Certificado X.509 de componente.

Zona privada accesible por el ciudadano con PIN

- Certificado de Firma, para la realización de firmas electrónicas.
- Certificado de Autenticación, para autenticación electrónica en Internet.

Zona de seguridad accesible en en los Puntos de Actualización

- Datos de filiación del ciudadano (los mismos que en el soporte físico).
- Imagen de la fotografía.
- Imagen de la firma manuscrita.

DNIe (III)
Mecanismo de seguridad

DNIe (III)
Mecanismo de seguridad

- Autenticación de los elementos para asegurar que la tarjeta ha sido emitida por la DGP.

DNIe (III)
Mecanismo de seguridad

- Autenticación de los elementos para asegurar que la tarjeta ha sido emitida por la DGP.
- Establecimiento de canal seguro que garantice la confidencialidad entre la tarjeta y el sistema.

DNIe (III)
Mecanismo de seguridad

- Autenticación de los elementos para asegurar que la tarjeta ha sido emitida por la DGP.
- Establecimiento de canal seguro que garantice la confidencialidad entre la tarjeta y el sistema.
- Protocolo de desafío-respuesta según la norma CWA 14890.

DNIe (III)
Mecanismo de seguridad

- Autenticación de los elementos para asegurar que la tarjeta ha sido emitida por la DGP.
- Establecimiento de canal seguro que garantice la confidencialidad entre la tarjeta y el sistema.
- Protocolo de desafío-respuesta según la norma CWA 14890.
- Permite al sistema policial determinar si el DNIe es legítimo y el establecimiento de un canal seguro entre las tarjetas y el software que accede.

DNIe (III)
Mecanismo de seguridad

- Autenticación de los elementos para asegurar que la tarjeta ha sido emitida por la DGP.
- Establecimiento de canal seguro que garantice la confidencialidad entre la tarjeta y el sistema.
- Protocolo de desafío-respuesta según la norma CWA 14890.
- Permite al sistema policial determinar si el DNIe es legítimo y el establecimiento de un canal seguro entre las tarjetas y el software que accede.
- Existen Hardware Security Modules (HSMs) policiales de la infraestructura de certificación correspondiente.

Contenido

Diseño del sistema

Diseño del sistema

- Aplicación móvil para dispositivos Android.

Diseño del sistema

- Aplicación móvil para dispositivos Android.
- Verificación de todos los mecanismos de seguridad (BAC, PA, EAC, AA) de MRTD utilizando CSCA y CVCA.

Diseño del sistema

- Aplicación móvil para dispositivos Android.
- Verificación de todos los mecanismos de seguridad (BAC, PA, EAC, AA) de MRTD utilizando CSCA y CVCA.
- Establecimiento de canal seguro de administración con el DNIe.

Diseño del sistema

- Aplicación móvil para dispositivos Android.
- Verificación de todos los mecanismos de seguridad (BAC, PA, EAC, AA) de MRTD utilizando CSCA y CVCA.
- Establecimiento de canal seguro de administración con el DNIe.
- Lectura de los datos de de los documentos.

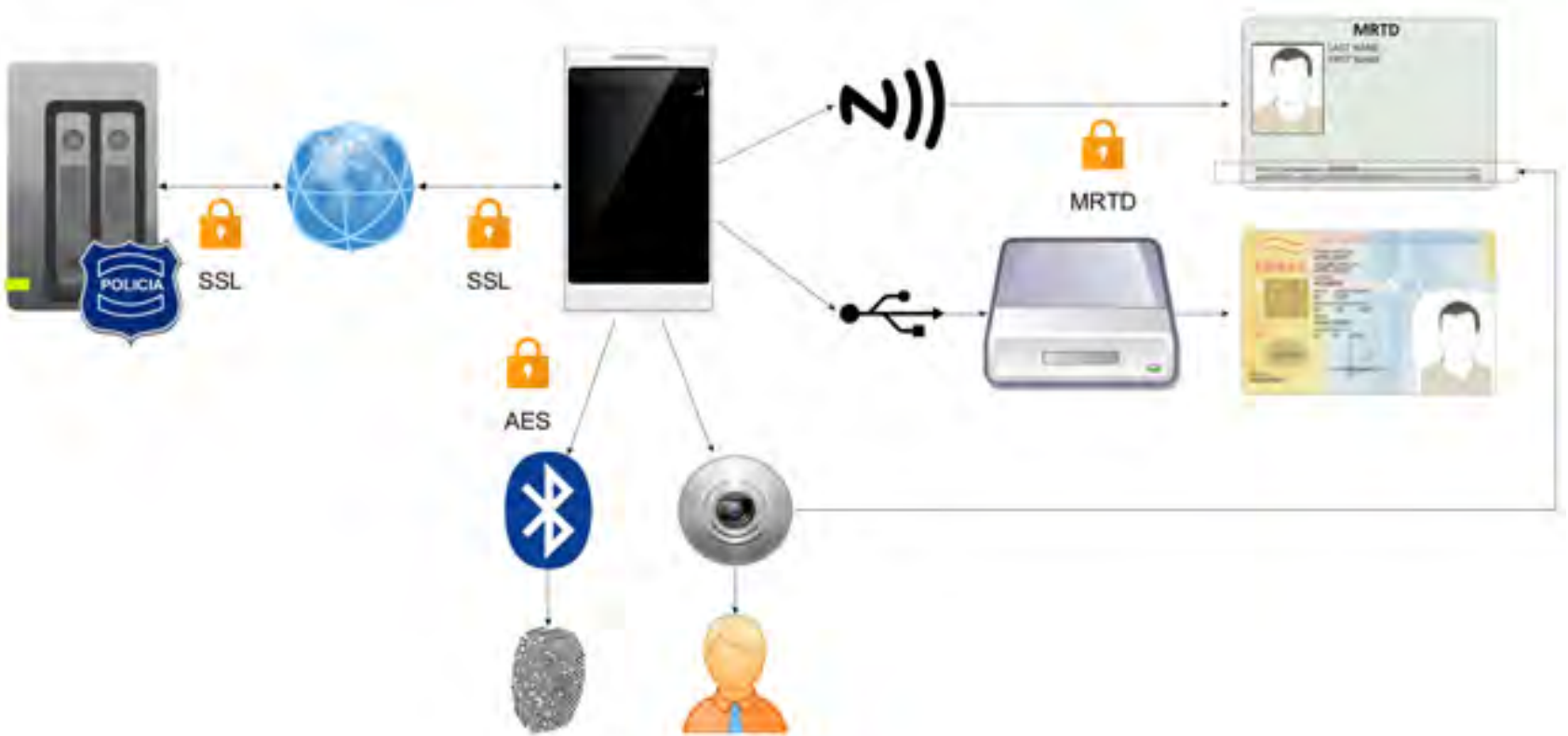
Diseño del sistema

- Aplicación móvil para dispositivos Android.
- Verificación de todos los mecanismos de seguridad (BAC, PA, EAC, AA) de MRTD utilizando CSCA y CVCA.
- Establecimiento de canal seguro de administración con el DNIe.
- Lectura de los datos de de los documentos.
- Validaciones contra sistemas policiales del titular y el documento.

Diseño del sistema

- Aplicación móvil para dispositivos Android.
- Verificación de todos los mecanismos de seguridad (BAC, PA, EAC, AA) de MRTD utilizando CSCA y CVCA.
- Establecimiento de canal seguro de administración con el DNIe.
- Lectura de los datos de de los documentos.
- Validaciones contra sistemas policiales del titular y el documento.
- Lectura y cotejo de elementos biométricos faciales y dactilares.

Diseño del sistema (II)
Componentes Hardware



Componentes Software
APIs diseñadas

- Componente general de utilidades generalistas y frecuentes (cadenas, arrays, codificaciones...).

- Componente general de utilidades generalistas y frecuentes (cadenas, arrays, codificaciones...).
- API de inspección de documentos (InspectionService).
  - Verificación de SOD (PA).
  - Verificación de cadenas y firma (EAC).

- Componente general de utilidades generalistas y frecuentes (cadenas, arrays, codificaciones...).
- API de inspección de documentos (InspectionService).
  - Verificación de SOD (PA).
  - Verificación de cadenas y firma (EAC).
- API de consulta de estado documentos (DSQService).

- Componente general de utilidades generalistas y frecuentes (cadenas, arrays, codificaciones...).
- API de inspección de documentos (InspectionService).
  - Verificación de SOD (PA).
  - Verificación de cadenas y firma (EAC).
- API de consulta de estado documentos (DSQService).
- API de consulta de antecedentes policiales (CRService).

- Componente general de utilidades generalistas y frecuentes (cadenas, arrays, codificaciones...).
- API de inspección de documentos (InspectionService).
  - Verificación de SOD (PA).
  - Verificación de cadenas y firma (EAC).
- API de consulta de estado documentos (DSQService).
- API de consulta de antecedentes policiales (CRService).
- API de captura dactilar (FingerprintReader).

Componentes Software (II)
Módulo Principal

Componentes Software (II)
Módulo Principal

- Proporciona la interfaz completa de usuario (Android).

Componentes Software (II)
Módulo Principal

- Proporciona la interfaz completa de usuario (Android).
- elegir modo de lectura:
  - Lector ICC conectado (DNIe).
  - OCR de la MRZ (MRTD).
  - BAC manual con número, fecha de nacimiento y de caducidad (MRTD).

Componentes Software (II)
Módulo Principal

- Proporciona la interfaz completa de usuario (Android).
- elegir modo de lectura:
  - Lector ICC conectado (DNIe).
  - OCR de la MRZ (MRTD).
  - BAC manual con número, fecha de nacimiento y de caducidad (MRTD).
- Verificación y lectura del documento:
  - BAC, PA, AA o EAC para MRTD.
  - Canal administrativo con el DNIe, autenticación mutua tarjeta/lector.

Componentes Software (II)
Módulo Principal

- Proporciona la interfaz completa de usuario (Android).
- elegir modo de lectura:
  - Lector ICC conectado (DNIe).
  - OCR de la MRZ (MRTD).
  - BAC manual con número, fecha de nacimiento y de caducidad (MRTD).
- Verificación y lectura del documento:
  - BAC, PA, AA o EAC para MRTD.
  - Canal administrativo con el DNIe, autenticación mutua tarjeta/lector.
- Lectura de datos generales, fotografía facial, huella, firma, certificados X.509 del DNIe.

Componentes Software (II)
Módulo Principal

- Proporciona la interfaz completa de usuario (Android).
- elegir modo de lectura:
  - Lector ICC conectado (DNIe).
  - OCR de la MRZ (MRTD).
  - BAC manual con número, fecha de nacimiento y de caducidad (MRTD).
- Verificación y lectura del documento:
  - BAC, PA, AA o EAC para MRTD.
  - Canal administrativo con el DNIe, autenticación mutua tarjeta/lector.
- Lectura de datos generales, fotografía facial, huella, firma, certificados X.509 del DNIe.
- Verificación policial de documento y titular (*DSQService* y *CRService*).

Componentes Software (II)
Módulo Principal

- Proporciona la interfaz completa de usuario (Android).
- elegir modo de lectura:
  - Lector ICC conectado (DNIe).
  - OCR de la MRZ (MRTD).
  - BAC manual con número, fecha de nacimiento y de caducidad (MRTD).
- Verificación y lectura del documento:
  - BAC, PA, AA o EAC para MRTD.
  - Canal administrativo con el DNIe, autenticación mutua tarjeta/lector.
- Lectura de datos generales, fotografía facial, huella, firma, certificados X.509 del DNIe.
- Verificación policial de documento y titular (*DSQService* y *CRService*).
- Captura facial (cámara trasera) y cotejo.

Componentes Software (II)
Módulo Principal

- Proporciona la interfaz completa de usuario (Android).
- elegir modo de lectura:
  - Lector ICC conectado (DNIe).
  - OCR de la MRZ (MRTD).
  - BAC manual con número, fecha de nacimiento y de caducidad (MRTD).
- Verificación y lectura del documento:
  - BAC, PA, AA o EAC para MRTD.
  - Canal administrativo con el DNIe, autenticación mutua tarjeta/lector.
- Lectura de datos generales, fotografía facial, huella, firma, certificados X.509 del DNIe.
- Verificación policial de documento y titular (*DSQService* y *CRService*).
- Captura facial (cámara trasera) y cotejo.
- Obtención de huellas (*FingerprintReader*) y cotejo.

Contenido

Implementación
Herramientas

Implementación
Herramientas

- Java, Android.

- Java, Android.
- Eclipse y Android Development Tools (ADT) para el desarrollo.

- Java, Android.
- Eclipse y Android Development Tools (ADT) para el desarrollo.
- Maven para dependencias, librerías, entregables y empaquetamiento.

- Java, Android.
- Eclipse y Android Development Tools (ADT) para el desarrollo.
- Maven para dependencias, librerías, entregables y empaquetamiento.
- Subversion para el control de versiones.

- Java, Android.
- Eclipse y Android Development Tools (ADT) para el desarrollo.
- Maven para dependencias, librerías, entregables y empaquetamiento.
- Subversion para el control de versiones.
- **MiKTEX**, **TEXnicCenter** y **JabRef** para la creación de memoria y presentación con LATEX.

Implementación (II)
Librerías de terceros

Implementación (II)
Librerías de terceros

- **jMRTD** y **SCUBA** para los estándares MRTD.

Implementación (II)
Librerías de terceros

- **jMRTD** y **SCUBA** para los estándares MRTD.
- **tess-two** y **Leptonica** para el procesamiento OCR.

Implementación (II)
Librerías de terceros

- **jMRTD** y **SCUBA** para los estándares MRTD.
- **tess-two** y **Leptonica** para el procesamiento OCR.
- **Neuro SDK** para los cotejos biométricos.

Implementación (II)
Librerías de terceros

- **jMRTD** y **SCUBA** para los estándares MRTD.
- **tess-two** y **Leptonica** para el procesamiento OCR.
- **Neuro SDK** para los cotejos biométricos.
- **slf4j** y**log4j** para la gestión de trazas.

Implementación (II)
Librerías de terceros

- **jMRTD** y **SCUBA** para los estándares MRTD.
- **tess-two** y **Leptonica** para el procesamiento OCR.
- **Neuro SDK** para los cotejos biométricos.
- **slf4j** y**log4j** para la gestión de trazas.
- **jmulticard (DNIDroid Inteco)**, para los accesos al DNIe.

Implementación (II)
Librerías de terceros

- **jMRTD** y **SCUBA** para los estándares MRTD.
- **tess-two** y **Leptonica** para el procesamiento OCR.
- **Neuro SDK** para los cotejos biométricos.
- **slf4j** y**log4j** para la gestión de trazas.
- **jmulticard (DNIDroid Inteco)**, para los accesos al DNIe.
- **KSoap2-android** y **Simple XML** para Web Services SOAP.

Implementación (II)
Librerías de terceros

- **jMRTD** y **SCUBA** para los estándares MRTD.
- **tess-two** y **Leptonica** para el procesamiento OCR.
- **Neuro SDK** para los cotejos biométricos.
- **slf4j** y**log4j** para la gestión de trazas.
- **jmulticard (DNIDroid Inteco)**, para los accesos al DNIe.
- **KSoap2-android** y **Simple XML** para Web Services SOAP.
- **Spongy Castle** para tareas criptográficas.

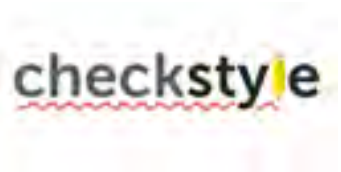
Contenido

Calidad de código y pruebas

Calidad de código y pruebas

- PMD, para el análisis de eficiencia y calidad del código.

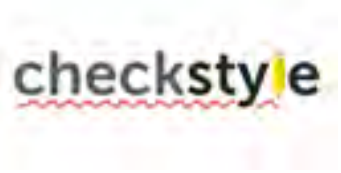
- Checkstyle (CS) para el control, estandarización, documentación y mejora de la calidad del código.



Calidad de código y pruebas

- PMD, para el análisis de eficiencia y calidad del código.

- Checkstyle (CS) para el control, estandarización, documentación y mejora de la calidad del código.



- reglas específicas definidas.

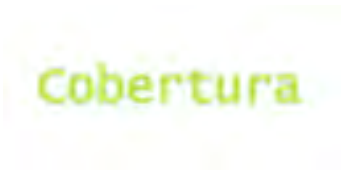
Calidad de código y pruebas

- PMD, para el análisis de eficiencia y calidad del código.

- Checkstyle (CS) para el control, estandarización, documentación y mejora de la calidad del código.

- reglas específicas definidas.

- Tests unitarios con JUnit en todas las librerías del proyecto.



- Chequeo con Cobertura para librería de utilidades comunes.

Contenido

Demostración...
Lectura de Pasaporte

ePasaporte
(NFC)

Demostración...
Lectura de DNIe

DNI 1.0

Contenido

Conclusiones

- Amplia evolución de los documentos de identificación y tránsito.
- Reducción del tamaño, precio, prestaciones y fiabilidad de periféricos.
- Tecnologías inalámbricas (NFC, Wi-Fi, Bluetooth) avanzadas.
- Escenarios avanzados de identificación rápida, segura y fiable.

Trabajo futuro

- Compatibilidad con PACE en nuevos MRTD.
- Compatibilidad con DNIe 3.0 por NFC (MRTD).
- Mecanismos de verificación física (marcas de agua, tintas IR o UV, etcétera.
- Mejoras de experiencia de usuario con estilos *Material Design*.
- Optimización de procesos asíncronos con alta carga de proceso.

Fin

Fin

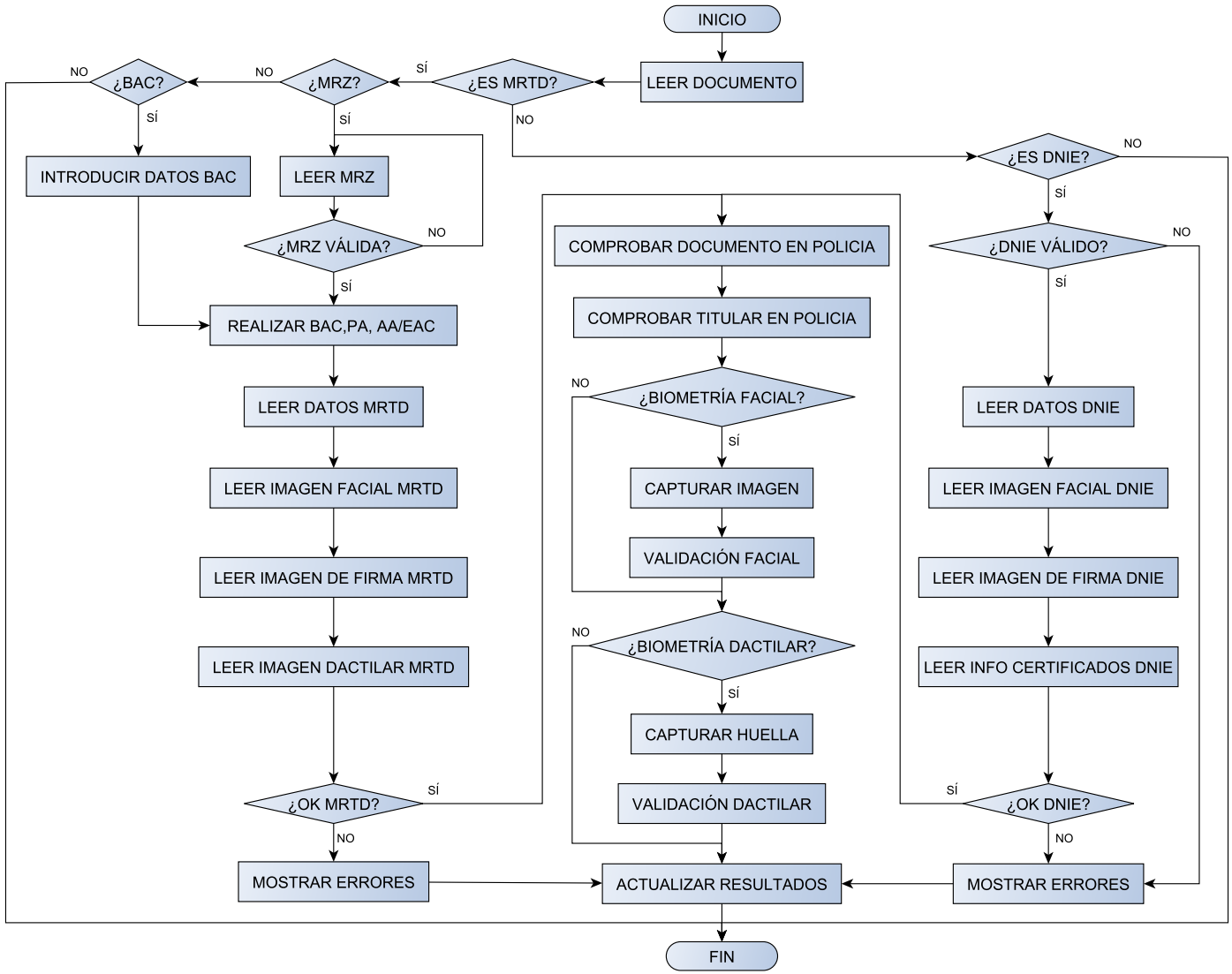
Preguntas...

Contenido

Diseño del sistema (III)
Componentes Hardware

- Smartphone Android en el que se desplegará la aplicación con:
  - Lector NFC para realizar las comunicaciones con los MRTD.
  - Cámara trasera para la captura de la MRZ y para la biometría facial.
  - USB OTG para acceder a las tarjetas ICC del DNIe.
  - Bluetooth para conectar con el lector de huellas.
  - Internet para conectar a sistemas policiales.
- Lector de huellas Bluefin mediante Bluetooth.

Componentes Software
Diagrama de Flujo



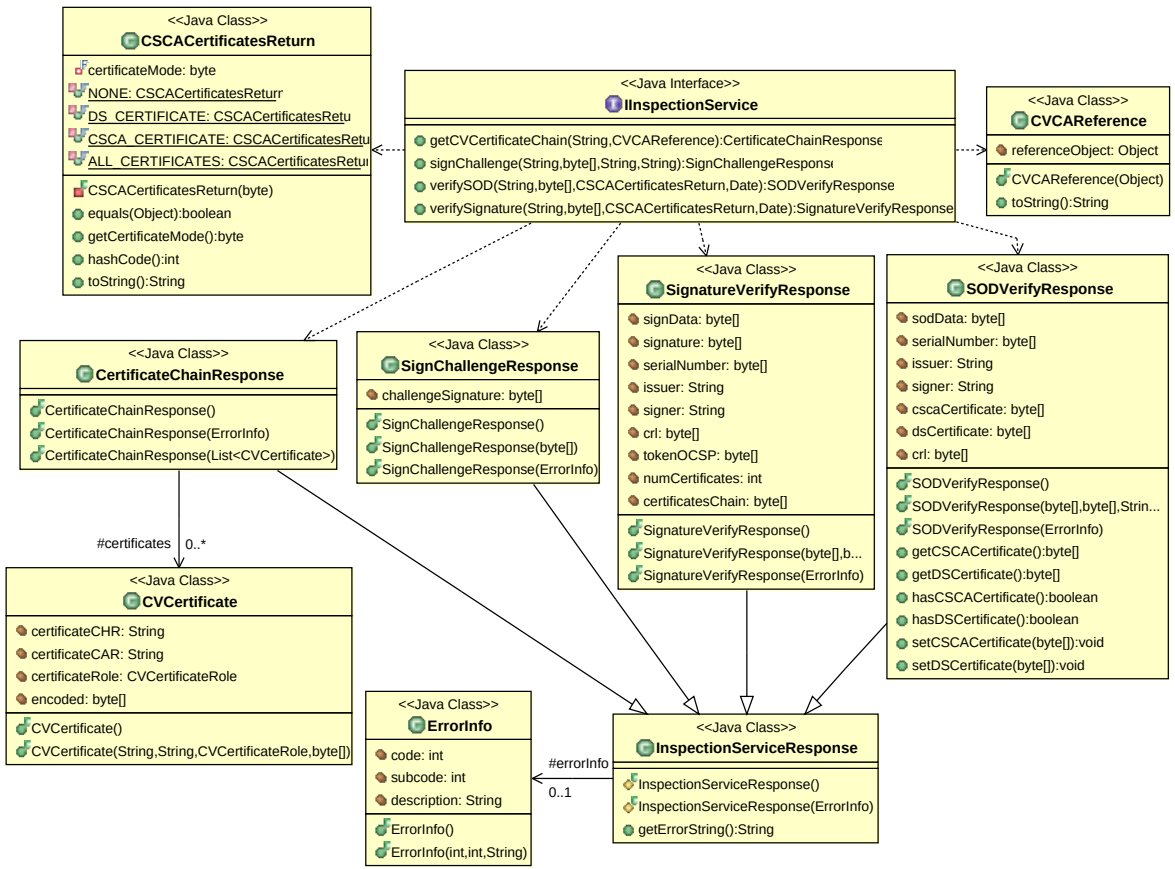
Componente general de utilidades generalistas y frecuentes.

- Utilidades de cadenas de caracteres o arrays.
- Utilidades base64 y hexadecimal.
- Utilidades certificados X.509.
- Utilidades de recursos y clases.
- Utilidades de listas y colecciones.
- Utilidades XML con Document Object Model (DOM).
- Utilidades de ficheros y procesos I/O.
- Utilidades numéricas.
- Utilidades de trazas.
- Utilidades HTTP, TLS, HTTPS, proxy, etcétera.

Componentes Software
API de inspección de documentos (InspectionService)

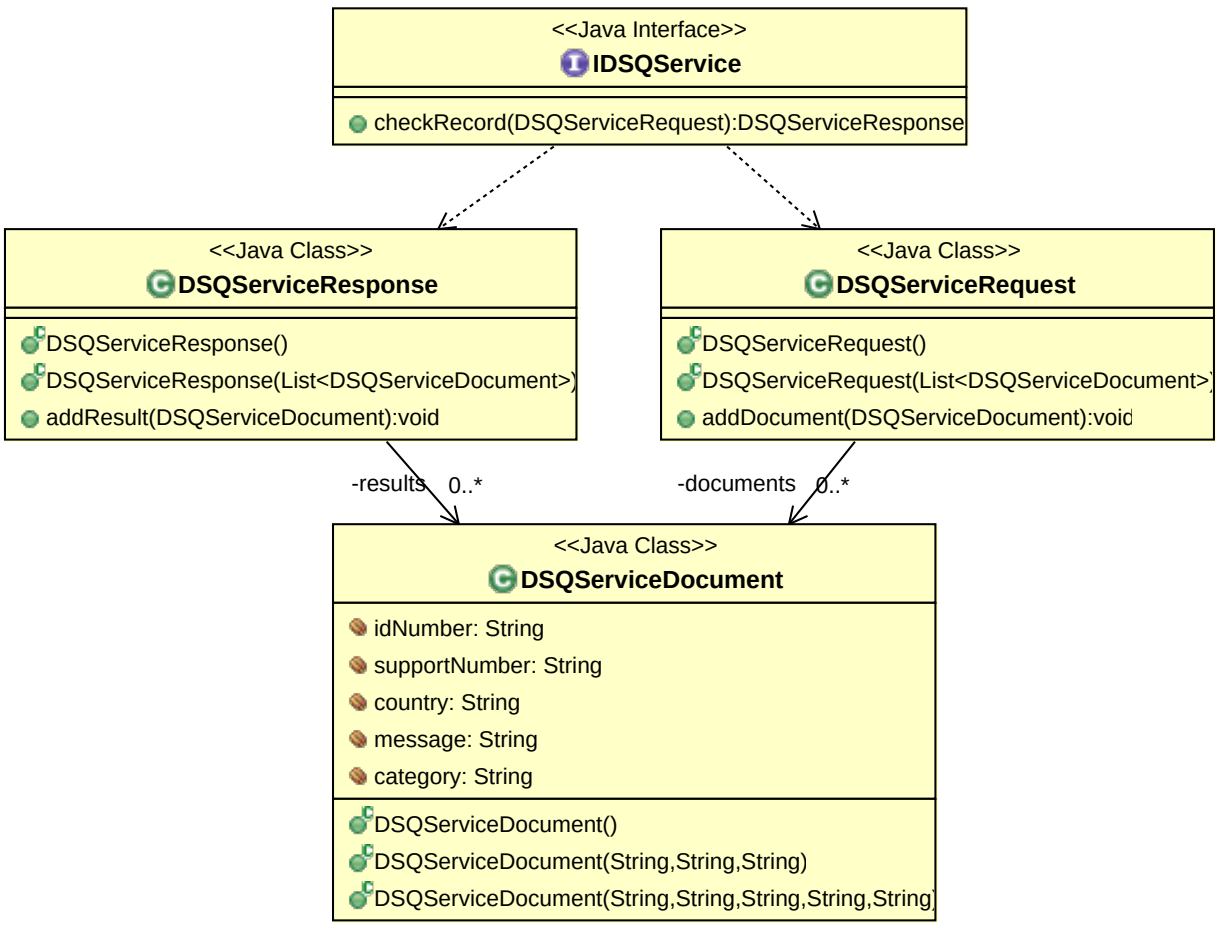
API para las tareas de inspección de documentos.

- Verificación de SOD (PA)
- Verificación de cadenas y firma (EAC).

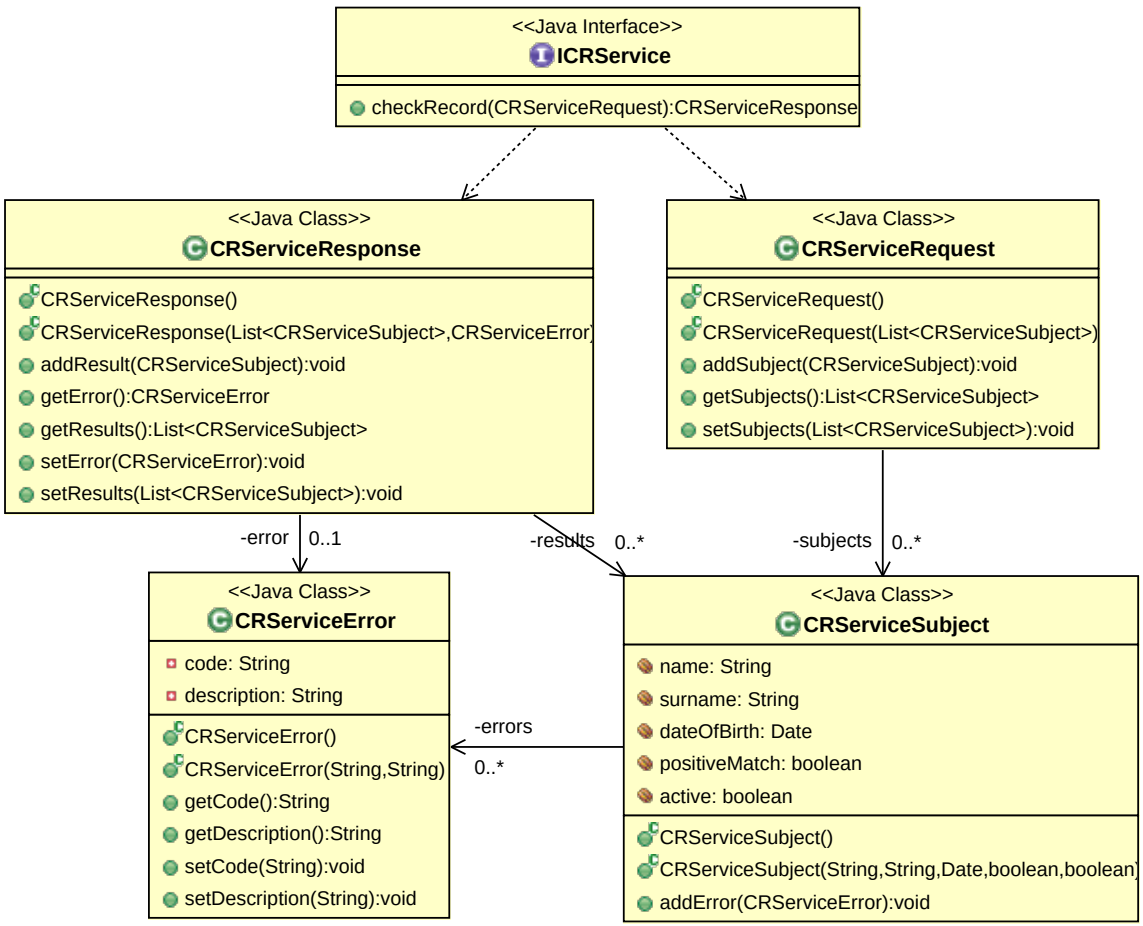


Componentes Software
API de consulta de documentos (DSQService)

API para consultas sobre estado policial de documentos.



API para consultas sobre señalamientos policiales de los titulares.



API de captura de la huella dactilar a través de lectores externos.